Federal Risk and Authorization Management Program (FedRAMP)

American Council for Technology
Industry Advisory Council
The Tower Club (Vienna, VA)

January 11, 2012

Agenda

Topic	Speaker
Overview of FedRAMP	Katie Lewin
Third Party Assessment Organizations (3PAO) Overview	Matt Goodrich
FedRAMP Security Controls & What's Next	Katie Lewin
Q&A Session	Panel
Closing Remarks	Dave McClure

What is FedRAMP?

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

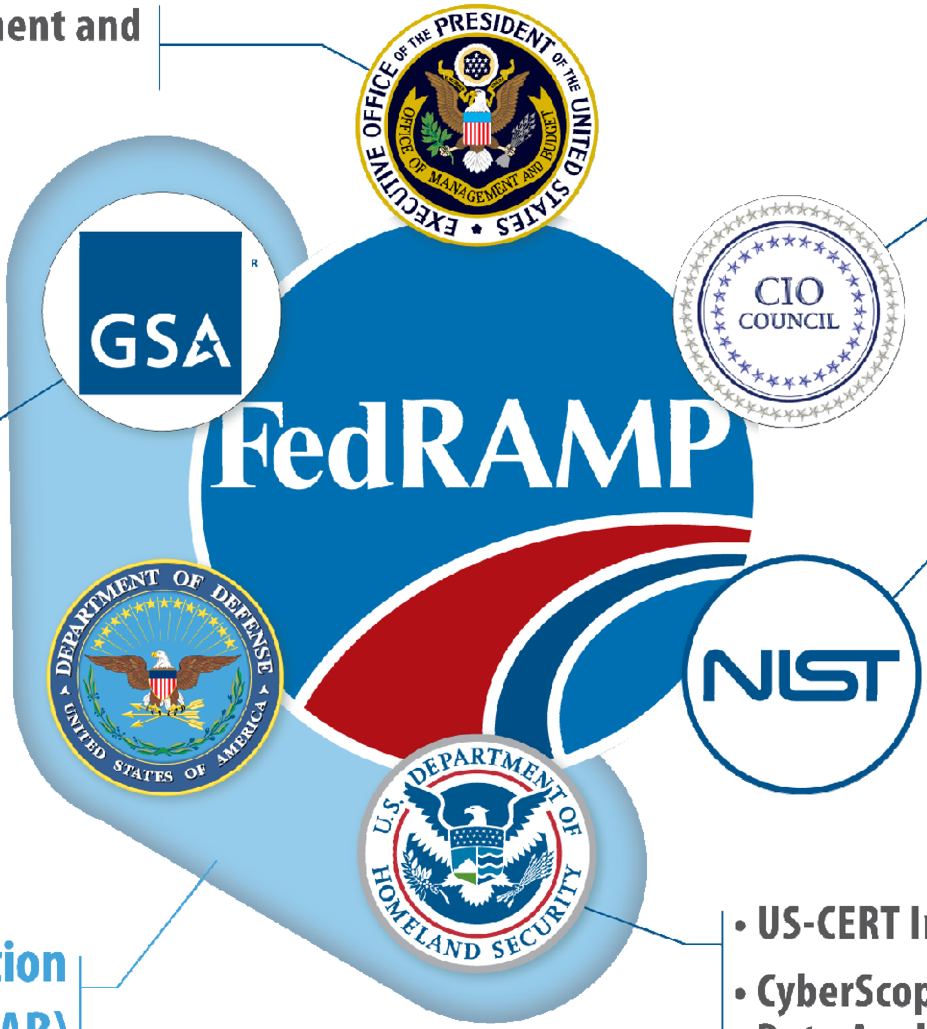
- This approach uses a “do once, use many times” framework that will save cost, time, and staff required to conduct redundant agency security assessments.

Key Benefits

- Re-use of existing security assessments across agencies
- Savings in cost, time and resources – do once, use many times
- Risk based not compliance based
- Transparency between government and cloud service providers
- Transparency → trust, reliability, consistency, and quality of the Federal security authorization process

Executive Sponsors

- Office of Management and Budget Policy


EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF MANAGEMENT AND BUDGET
GSA
CIO COUNCIL
FedRAMP
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
NIST
U.S. DEPARTMENT OF HOMELAND SECURITY

- ISIMC Guidance
- Cross Agency Coordination

- FedRAMP PMO

- FISMA Standards
- Technical Advisors
- Technical Specifications

- US-CERT Incident Coordination
- CyberScope Continuous Monitoring Data Analysis

Joint Authorization Board (JAB)

Major Players

Federal Agencies

JAB (DOD, DHS, GSA)
PMO- GSA
Technical Advisor – NIST
Continuous Monitoring - DHS

FedRAMP PMO

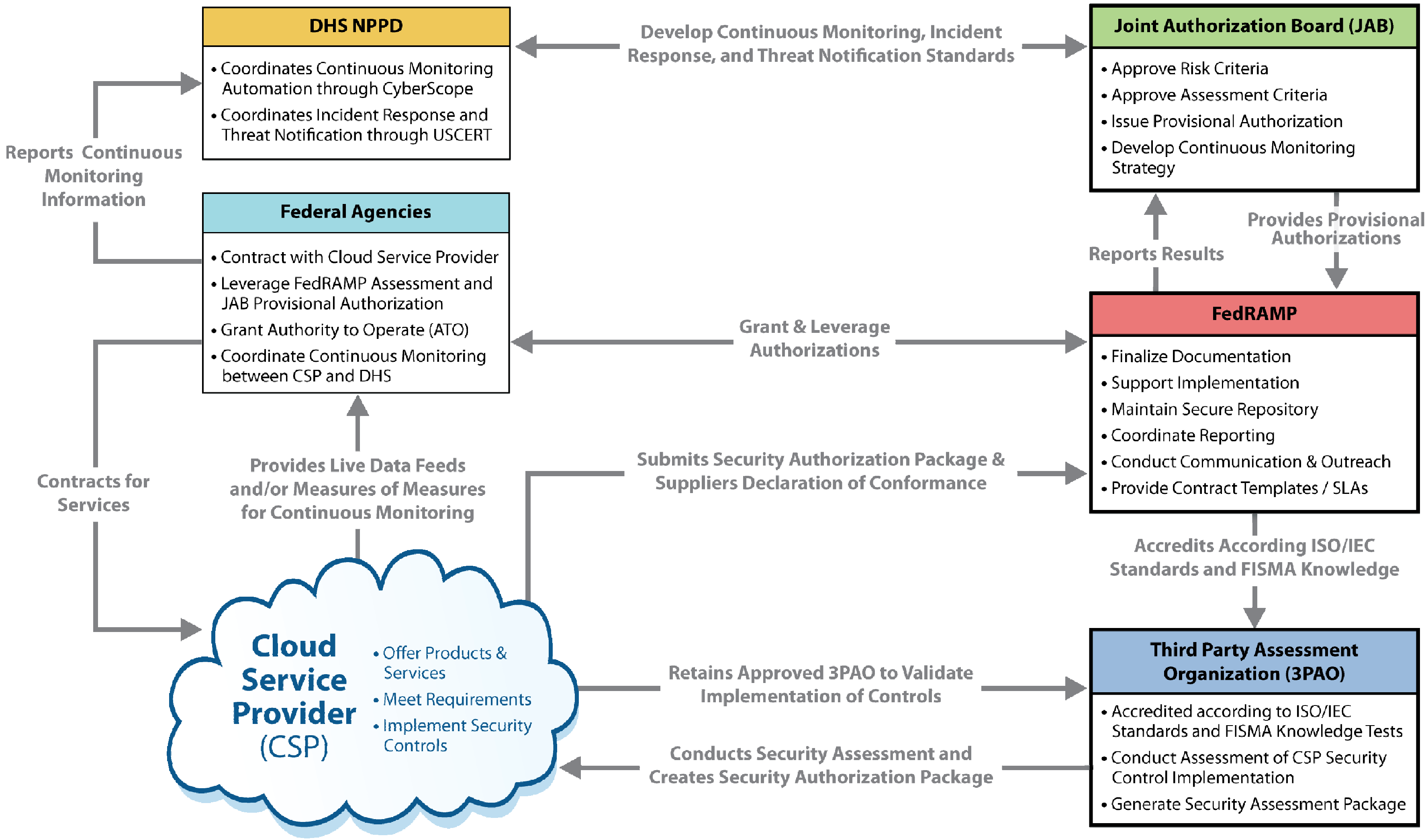
Cloud Service Provider

Provides Cloud IT Services with a provisional authorization granted by FedRAMP JAB

3rd Party Assessment Organization

Performs initial and periodic assessment of security and privacy controls deployed in Cloud information systems

FedRAMP Stakeholder Roles and Interaction



DHS NPPD

- Coordinates Continuous Monitoring Automation through CyberScope
- Coordinates Incident Response and Threat Notification through USCERT

Develop Continuous Monitoring, Incident Response, and Threat Notification Standards

Joint Authorization Board (JAB)

- Approve Risk Criteria
- Approve Assessment Criteria
- Issue Provisional Authorization
- Develop Continuous Monitoring Strategy

Reports Continuous Monitoring Information

Federal Agencies

- Contract with Cloud Service Provider
- Leverage FedRAMP Assessment and JAB Provisional Authorization
- Grant Authority to Operate (ATO)
- Coordinate Continuous Monitoring between CSP and DHS

Reports Results

Provides Provisional Authorizations

Grant & Leverage Authorizations

FedRAMP

- Finalize Documentation
- Support Implementation
- Maintain Secure Repository
- Coordinate Reporting
- Conduct Communication & Outreach
- Provide Contract Templates / SLAs

Contracts for Services

Provides Live Data Feeds and/or Measures of Measures for Continuous Monitoring

Submits Security Authorization Package & Suppliers Declaration of Conformance

Accredits According ISO/IEC Standards and FISMA Knowledge

Cloud Service Provider (CSP)

- Offer Products & Services
- Meet Requirements
- Implement Security Controls

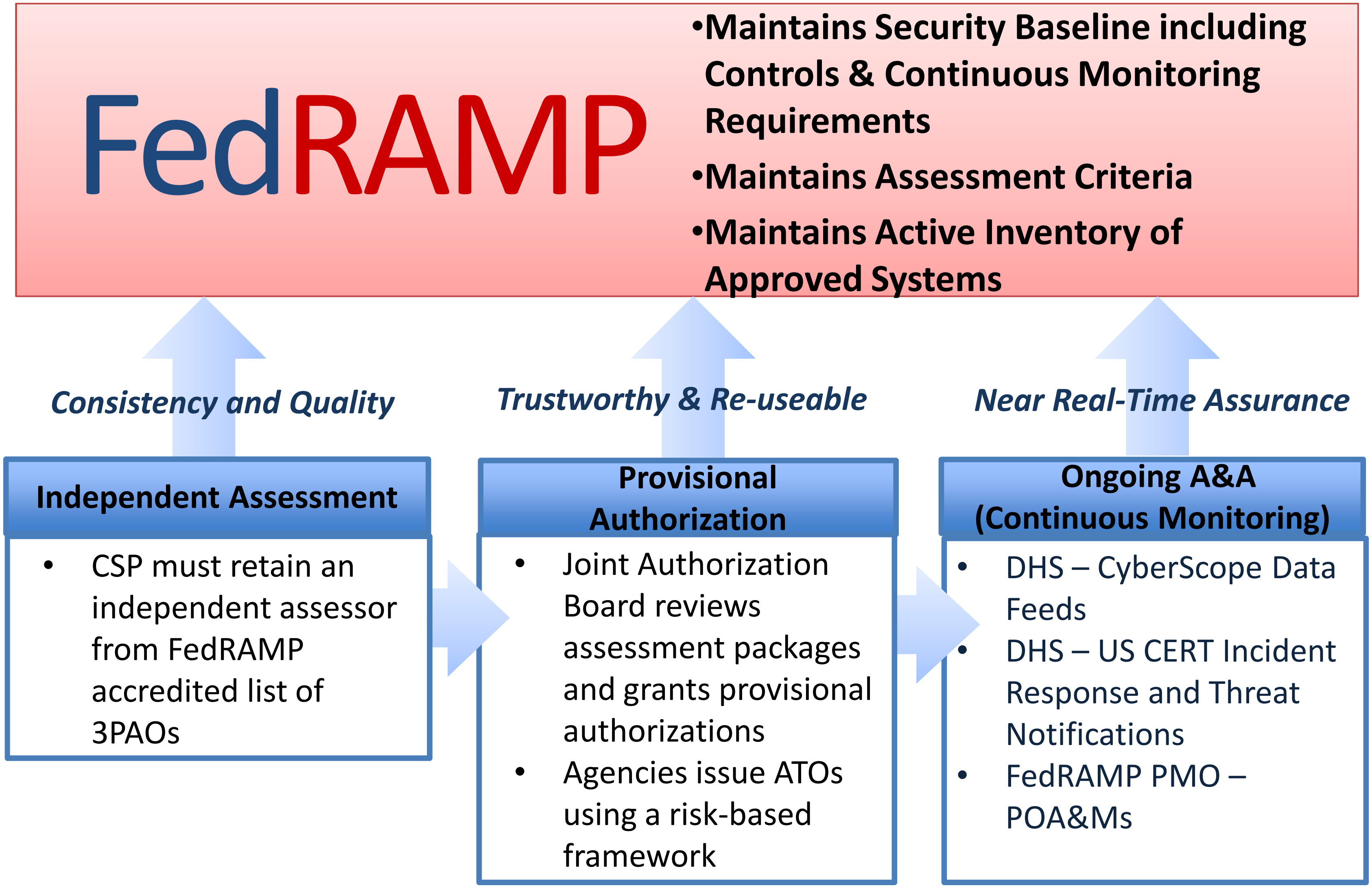
Retains Approved 3PAO to Validate Implementation of Controls

Conducts Security Assessment and Creates Security Authorization Package

Third Party Assessment Organization (3PAO)

- Accredited according to ISO/IEC Standards and FISMA Knowledge Tests
- Conduct Assessment of CSP Security Control Implementation
- Generate Security Assessment Package

FedRAMP and the Security Assessment and Authorization Process



FedRAMP

- Maintains Security Baseline including Controls & Continuous Monitoring Requirements
- Maintains Assessment Criteria
- Maintains Active Inventory of Approved Systems

Consistency and Quality

Trustworthy & Re-useable

Near Real-Time Assurance

Independent Assessment

- CSP must retain an independent assessor from FedRAMP accredited list of 3PAOs

Provisional Authorization

- Joint Authorization Board reviews assessment packages and grants provisional authorizations
- Agencies issue ATOs using a risk-based framework

Ongoing A&A (Continuous Monitoring)

- DHS – CyberScope Data Feeds
- DHS – US CERT Incident Response and Threat Notifications
- FedRAMP PMO – POA&Ms

FedRAMP Phases and Timeline

Phased evolution towards sustainable operations allows for the management of risks, capture of lessons learned, and incremental rollout of capabilities

	FY12	FY12	FY13 Q2	FY14
	Pre-Launch Activities	**Initial Operational Capabilities (IOC)**	**Full Operations**	**Sustaining Operations**
	Finalize Requirements and Documentation in Preparation of Launch	*Launch IOC with Limited Scope and Cloud Service Provider (CSP)s*	*Execute Full Operational Capabilities with Manual Processes*	*Move to Full Implementation with On-Demand Scalability*
Key Activities	• Publish FedRAMP Requirements (Security Controls, Templates, Guidance) • Publish Agency Compliance Guidance • Accredit 3PAOs • Establish Priority Queue	• Authorize CSPs • Update CONOPS, Continuous Monitoring Requirements and CSP Guidance	• Conduct Assessments & Authorizations • Scale Operations to Authorize More CSPs	• Implement Electronic Authorization Repository • Scale to Steady State Operations
Outcomes	• Initial List of Accredited 3PAOs • Launch FedRAMP into Initial Operating Capabilities	• Initial CSP Authorizations • Established Performance Benchmark	• Multiple CSP Authorizations • Defined Business Model • Measure Benchmarks	• Authorizations Scale by Demand • Implement Business Model • Self-Sustaining Funding Model Covering Operations • Privatized Accreditation Board

Gather Feedback and Incorporate Lessons Learned

Third Party Assessment Organizations (3PAO)

Matthew Goodrich
FedRAMP Program Manager
GSA Office of Citizen Services and Innovative Technologies

3PAO Responsibilities

- 3PAO = Cloud IT Security Auditor
- 3 main roles
  - Conduct Assessment of CSP Security Control Implementation
  - Generate Security Assessment Package
  - Perform initial and periodic security assessment of cloud information systems.

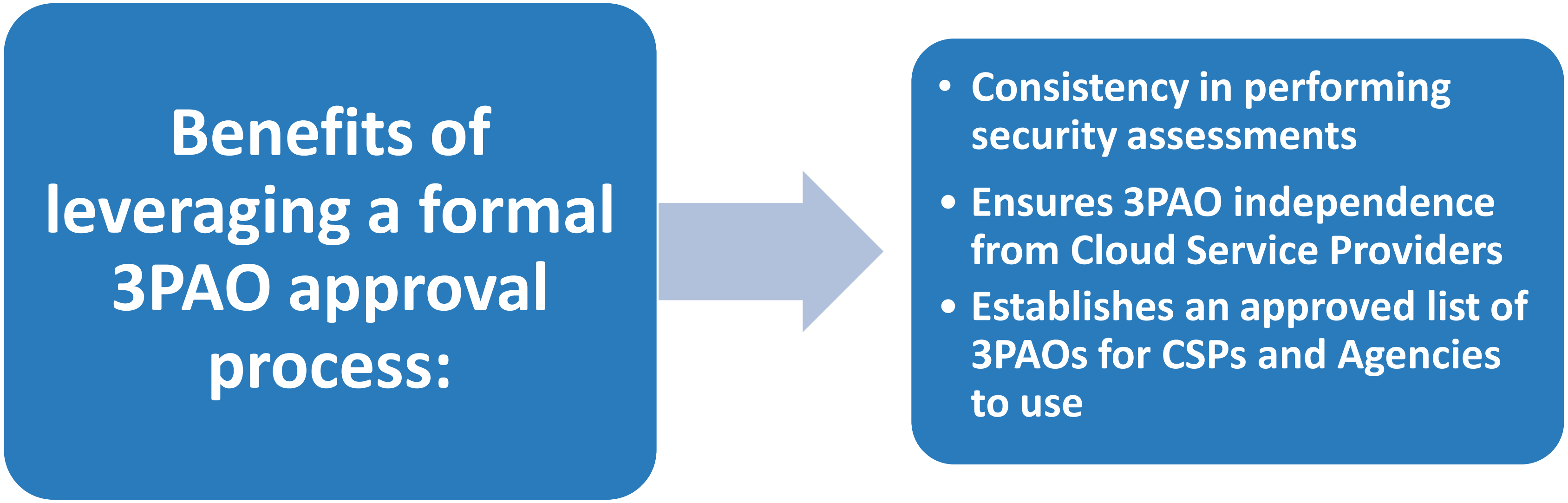
3PAO Conformity Assessment Process

FedRAMP requires CSPs to use Third Party Assessment Organizations (3PAOs) to independently validate and verify that they meet FedRAMP security requirements

Conformity assessment process to accredit 3PAOs based on NIST program

Conformity assessment process accredits 3PAOs based on:

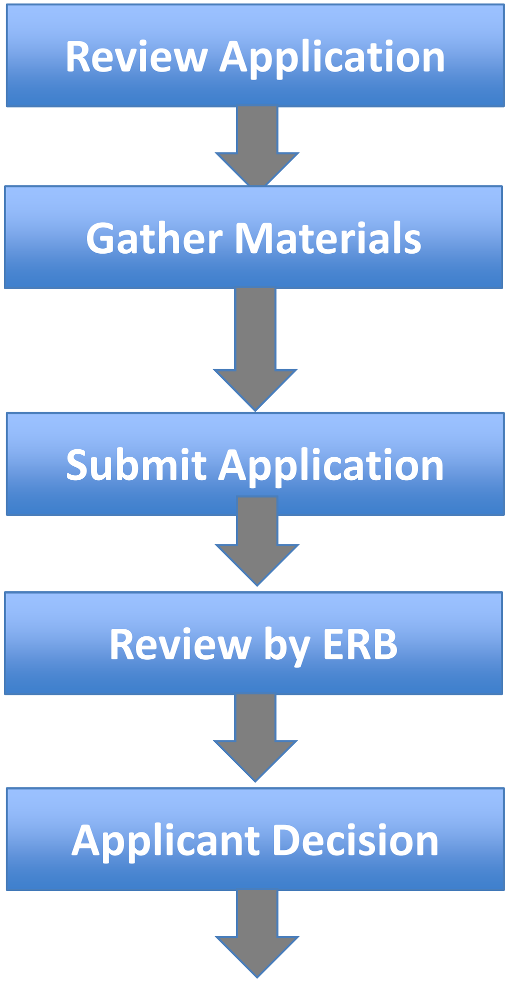
(1) Independence and quality management in accordance with ISO standards; and
(2) Technical competence through FISMA knowledge testing.



Benefits of leveraging a formal 3PAO approval process:

- **Consistency in performing security assessments**
- **Ensures 3PAO independence from Cloud Service Providers**
- **Establishes an approved list of 3PAOs for CSPs and Agencies to use**

3PAO Acceptance Process



Review Application

- 3PAO candidate reviews application at **www.FedRAMP.gov**; business decision to apply.

Gather Materials

- 3PAO candidate gathers artifacts and completes application

Security Assessment Report	**System Security Plan**	**Applicant Assessment Test Procedures**

Submit Application

- 3PAO candidate submits application

Review by ERB

- Expert Review Board with members from GSA and ISO independent cybersecurity experts review the application.

Applicant Decision

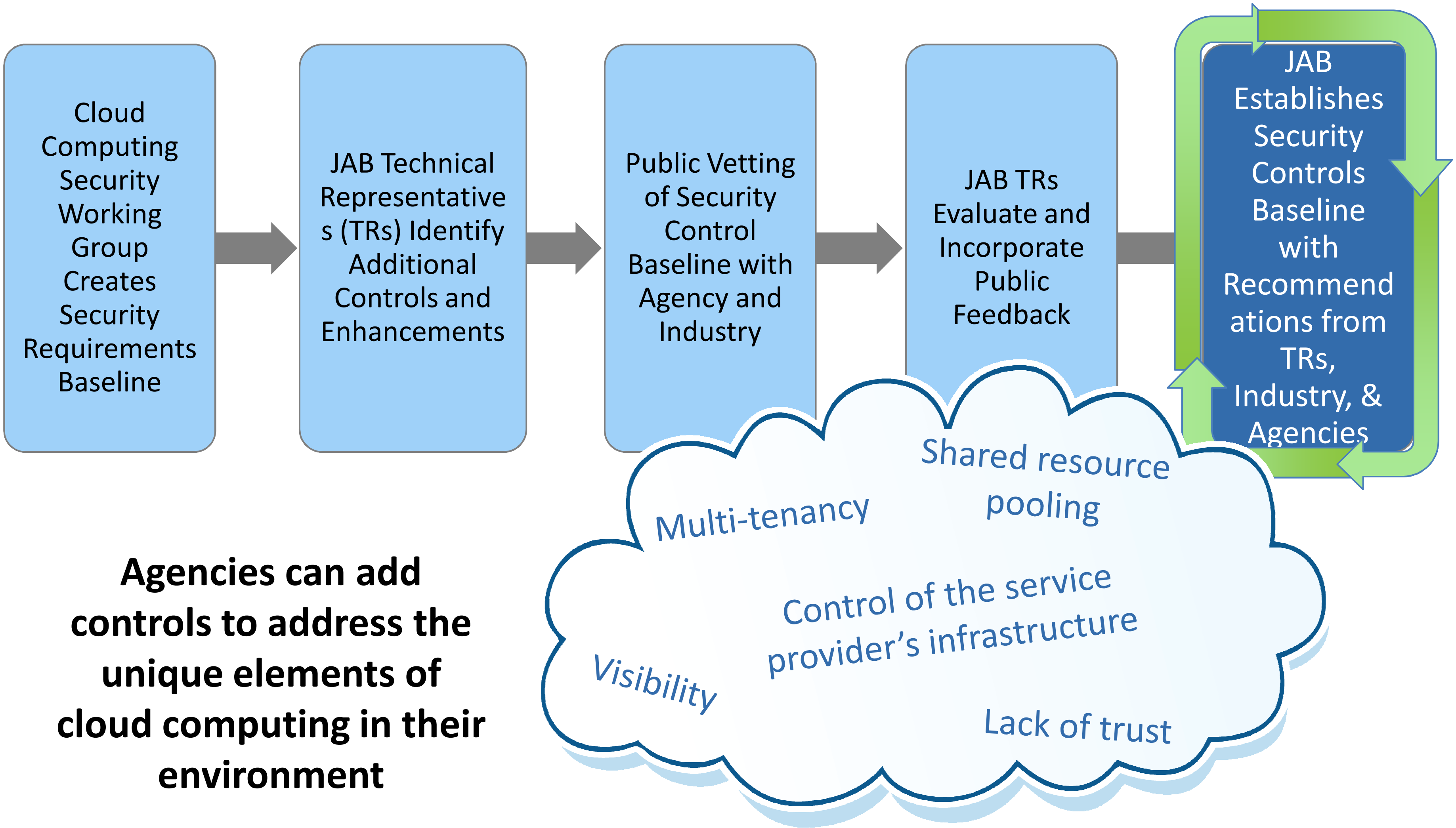
- FedRAMP PMO reviews ERB recommendation and provides 3PAO an acceptance decision.

List of Accredited 3PAO for Use by Agency and CSPs

FedRAMP Security Controls

Establishing Baseline FedRAMP Security Controls

Source of controls - NIST SP 800-53 R3 for low and moderate impact systems


Cloud Computing Security Working Group Creates Security Requirements Baseline
JAB Technical Representatives (TRs) Identify Additional Controls and Enhancements
Public Vetting of Security Control Baseline with Agency and Industry
JAB TRs Evaluate and Incorporate Public Feedback
JAB Establishes Security Controls Baseline with Recommendations from TRs, Industry, & Agencies
Shared resource pooling
Multi-tenancy
Control of the service provider's infrastructure
Visibility
Lack of trust

Agencies can add controls to address the unique elements of cloud computing in their environment

Security Controls

See FedRAMP.gov for list of security controls

Impact level	NIST Baseline Controls	Additional FedRAMP Controls	Total Controls Agreed to By JAB for FedRAMP
Low	115	1	116
Moderate	252	45	297

Areas with additional controls

Access Control (6)	Audit and Accountability (5)	Security Assessment and Authorization (1)	Configuration Management (4)
Contingency Planning (2)	Identification and Authentication (3)	Incident Response (1)	Maintenance (1)
Media Protection (1)	Risk Assessment (4)	System and Services Acquisition (4)	System and Communications Protection (11)
System and Information Integrity (1)			

Fully Implemented Control Examples

Risk Acceptability Criteria:

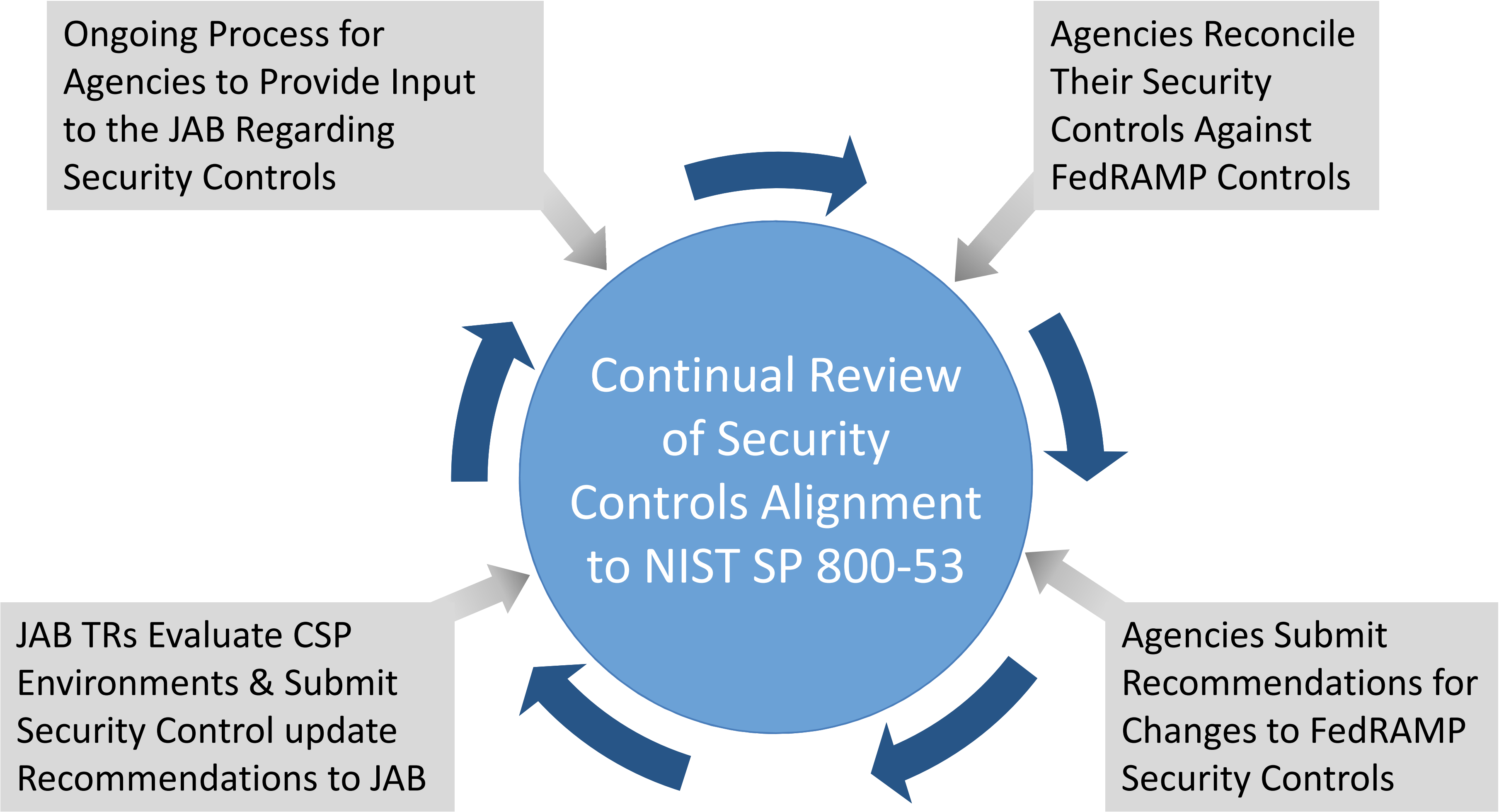
- controls that must be fully implemented – or risk level is unacceptable for CSP risk posture
- established by JAB
- relate to OMB Policy Memos, NIST Special Publications, or other Federal mandates

Examples:

Description***	Rationale	Associated Controls
Two Factor Authentication for access	Provides additional assurance that the user has been identified and authentication.	IA-2 (1) (2) (3)
Incident Handling and Incident Reporting consistent with Federal Guidelines	CSPs must support agency needs in handling and reporting incidents.	IR-4, IR-6
Boundary protection and effective separation of logical and physical devices within the authorization boundary	All points surrounding the accreditation boundary must be identified and protected.	SC-7

****The three criteria listed are not comprehensive. The risk acceptability criteria will be made publicly available once finalized by the JAB.*

Maintenance of Security Controls



Ongoing Process for Agencies to Provide Input to the JAB Regarding Security Controls

Agencies Reconcile Their Security Controls Against FedRAMP Controls

Continual Review of Security Controls Alignment to NIST SP 800-53

Agencies Submit Recommendations for Changes to FedRAMP Security Controls

JAB TRs Evaluate CSP Environments & Submit Security Control update Recommendations to JAB

What's Next

Activity	Date
3PAO Applications End for Initial Batch*	January 20, 2012 at 5pm EST
FedRAMP CONOPS Release	February 5, 2012
Release of Initial List of 3PAOs	March – April 2012
Launch FedRAMP Initial Operating Capabilities	June 2012
Initial CSP Authorizations	Q4 2012, Q1 2013

*After initial batch, applications for 3PAOs processed on an ongoing basis.

For more information, please contact us or visit us at any of the following websites:

www.FedRAMP.gov
www.gsa.gov/FedRAMP
Follow us on twitter @ FederalCloud